EU General Data Protection Regulation

A survival guide for private equity

Hogan Lovells

Introduction

Time to prepare

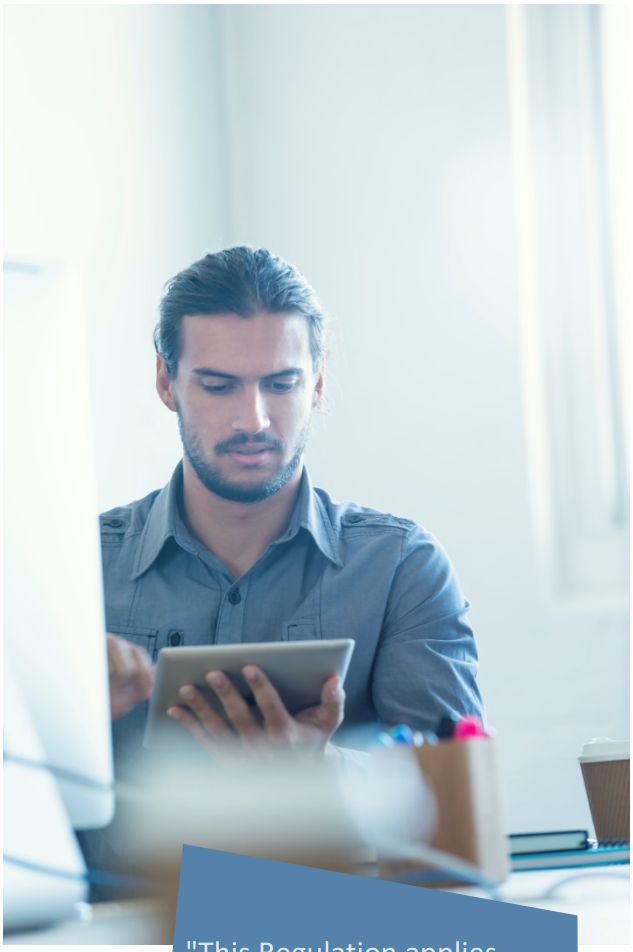
To say that the EU General Data Protection Regulation (GDPR or the Regulation) will change the existing data protection framework in Europe is an understatement. In less than a year, an ambitious, complex and strict law will transform the way in which personal information is collected, shared and used globally.

It is fair to say that the GDPR aims to take data protection compliance to a new level. Therefore, it is essential that we appreciate what is significant about the GDPR in relation to both private equity funds and the companies they invest in.

The Regulation will apply in all Member States from 25 May 2018 and therefore the time to start preparing is now. The changes to the existing regime present a good opportunity to refocus on and improve the way your organisation manages personal data. Remember too that with new steeper fines for failure to comply with the GDPR, you should ignore your portfolio companies' compliance at your peril – such significant fines could cause serious diminution in portfolio values.

Not just for European private equity

It would be incorrect to assume that the GDPR will not apply to non-European private equity houses. Where the individual to whom the relevant data relates (the data subject) is a European individual, and your firm controls and is responsible for the data that it holds in connection with that data subject, you, as a data controller, will need to comply with the new European rules. So, for non-European private equity houses with employees operating out of an EU Member State or with individual European investors investing in the firm's managed funds, an understanding of the new Regulation is necessary. Similarly, non-European funds investing in portfolio companies either seated in Europe or with data subjects in Europe, will need to understand the implications of the GDPR for those investments and the effect that any breach might have on them. Even though a private equity firm will not be directly responsible for their portfolio companies' compliance with the GDPR, it cannot be under-estimated how the new higher penalties could impact the value of a portfolio.



"This Regulation applies to the processing of data subjects who are in the Union by a controller or processor not established in the Union..." Article 3

Things you should know about the EU General Data Protection Regulation

"…make no mistake, this one's a game changer for everyone."

Elizabeth Denham
(Information Commissioner)

Geographical applicability

A very carefully thought out aspect of the GDPR is its geographical applicability – both within and outside the EU. For starters, the GDPR will be directly applicable across all Member States of the EU without any further intervention from the national parliaments. One of the main flaws of the original Directive was that it had to be implemented by national legislation in order to become law. That led to a patchwork of obligations that were not identical across the EU and caused a lack of harmonisation.

An effective move to address this problem was to change the format of the law altogether and adopt a single and all-encompassing regulation. Therefore, on paper at least, having a single law will provide much needed consistency, although it will still be interpreted in accordance with national approaches and idiosyncrasies.

Beyond Europe, the applicability of the GDPR to private equity firms without an establishment in the EU will be determined by the location of their data subjects. Those data subjects will include employees operating in European offices and individual European fund investors. Similarly, non-EU portfolio companies with employees or customers in Europe will be subject to the GDPR where personal data is collected from those individuals.

To this effect, the GDPR will apply whenever the use of personal data by the private equity firm or portfolio company relates to:

- the offering of goods or services (including investment services) to individuals in the EU, irrespective of whether a payment is required, or
- the monitoring of those individuals' behaviour in the EU.

The GDPR also clarifies that tracking individuals on the Internet to analyse or predict their personal preferences – as many websites and apps do – will trigger the application of the EU law. This measure makes almost every website that drops tracking cookies or apps that retrieve usage information, subject to the GDPR. This may not be a particular issue for private equity firms themselves but will have direct applicability when conducting due diligence on, or preparing for sale, any portfolio entity operating a technology or web based business.

Putting people in control

Something important to understand at the outset is the overall aim underpinning the GDPR: putting people in control of their data, whether that is your employees, your investors, your co-investors, or the customers or employees of your portfolio companies. This is a theme that is present throughout the text of the Regulation and is emphasised by the strengthening of 'consent' in relation to the use of data. When relied upon as a justification for the use of data, consent will need to meet very high standards and satisfy certain criteria. For example:

- consent cannot be bundled with T&Cs without clearly distinguishing between the uses of personal data and the other matters governed by the T&Cs;
- consent must be capable of withdrawal at any time and in an easy way that

should be explained to data subjects before it is obtained; and

- if consent is presented as 'take it or leave it' it may not be regarded as freely given.

Individuals' control over their data will also be subject to significantly reinforced rights, including:

- the requirement to provide information about data use to individuals at the point of data collection or within a reasonable period afterwards;
- a right of access to the data for the data subject;
- a right to rectification of inaccurate data;
- a right to erasure (also known as 'right to be forgotten');
- a right to restriction of processing;
- a right to data portability;
- a right to object to the processing altogether; and
- a right not to be subject to a decision based solely on automated processing.

Transparency, erasure and portability in particular are likely to emerge as crucial tools for individuals to use in the face of an ever growing hunger for our digital data. These rights will become more meaningful than ever before, so a greater uptake than until now should be expected. As such, this should be a particular watch point when conducting due diligence, particularly diligence of those businesses that are heavily web-based.

The big novelty: Accountability obligations

From a practical perspective, one of the most notable novelties of the GDPR is the requirement to make businesses more accountable for their data practices. This will be where private equity is likely to be affected the most since data processing is not typically a primary function and therefore accountability in connection with data protection may not have been a priority. Brand new responsibilities include:

- the implementation of data protection policies;
- data protection by design and data protection by default;
- record keeping obligations by controllers and any other person (other than your employees) who processes data on your behalf (processors);
- co-operation with supervisory authorities by controllers and processors;
- data protection impact assessments;
- prior consultation with data protection authorities in high-risk cases; and
- mandatory data protection officers for controllers and processors within the public sector and those undertaking Big Data processing activities.

On the data security front, there are additional highlights:

- Under the Regulation there are extremely detailed requirements for controllers to impose contractually onto vendors acting as processors – from a day to day compliance perspective, this will be one of the toughest challenges, particularly when engaging cloud services or any of the off-the-shelf solutions on which every business relies to communicate and store data. For private equity, this will include the use of cloud and networked data rooms used in

investment and divestment due diligence.

- Data breach notification to data protection authorities must be made within 72 hours of spotting an incident – this obligation does not apply if there is no risk for individuals, but if the risk is high, controllers and processors will need to notify the individuals as well.

Crucially, the GDPR does not limit its accountability obligations to controllers. Many of these new requirements apply equally to processors. This is a major practical difference between the GDPR and the existing Directive, which highlights the new focus on compliance across all roles within the information life-cycle. For private equity this means that, not only will firms need to be alert to the requirements of the GDPR when acting as a data controller in respect of their employees and investors, but also when 'processing' information and data received when diligencing potential targets. Similarly, when engaging third party advisers or service providers to support auction and sale processes in connection with portfolio divestments, contracts with those third party providers will need to include appropriate provisions which meet the requirements of the GDPR where they are processing data on your behalf.

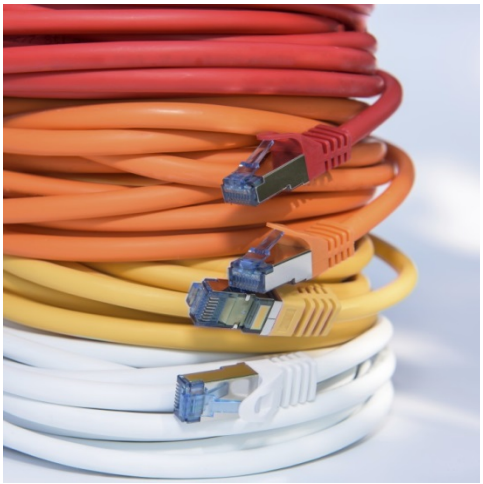
Still restrictions on international data transfers

As counter-intuitive as it may seem to regulate cross-border data flows in the 21st century, the GDPR carries on with the traditional approach to restrict data transfers to non-EU jurisdictions. Aside from transfers to jurisdictions that are officially declared by the European Commission to be adequate, both controllers and processors may only transfer personal data outside the EU if they put in place appropriate safeguards and on condition that enforceable rights and effective legal remedies for individuals are available.

The GDPR has helpfully expanded the range of measures that may be used to legitimise such transfers, which now include:

- binding corporate rules (BCR);
- standard contractual clauses (SCC) adopted by the European Commission;
- standard contractual clauses adopted by a data protection authority and approved by the European Commission;
- an approved code of conduct;
- an approved certification mechanism;
- other contractual clauses authorised by a data protection authority in accordance with the so-called 'consistent mechanism'.

Some of these, such as the SCC, have been tested over the years, so their benefits and limitations are well known. Others will need some time to show their value and effectiveness. For example, ad-hoc contractual clauses may become a more realistic solution than SCC, but they are likely to require a greater amount of effort in terms of drafting and interaction with regulators. What is patently clear is the growing support for BCR by law makers and regulators, but BCR should be seen as a framework for global privacy compliance more than a simple mechanism to overcome transfer restrictions.



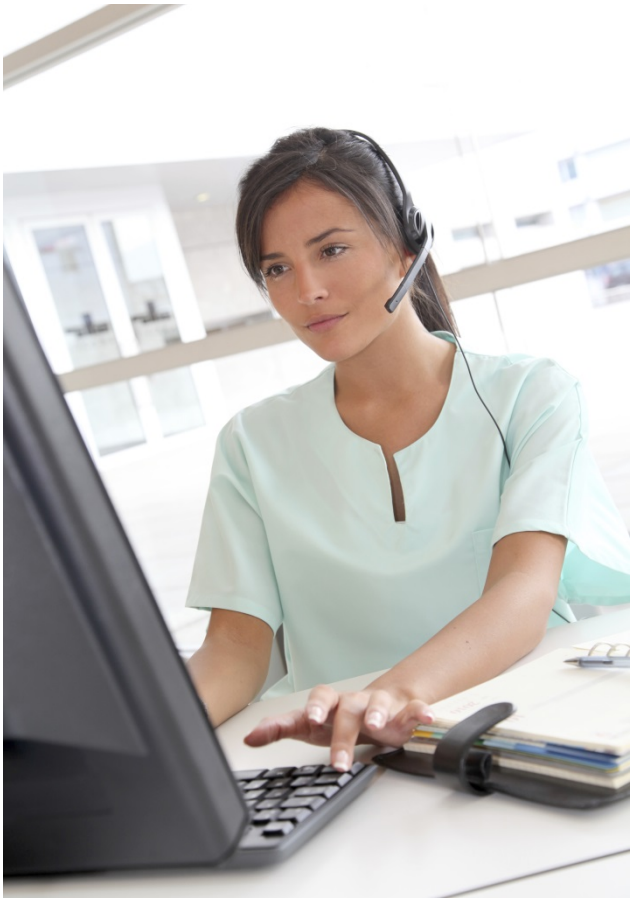
To comply or not to comply

When faced with such a complex and strict framework, an inevitable question always is: What is the risk of non-compliance? This question might be seen as an acknowledgment that 100% compliance is not achievable and that getting things right is going to involve a degree of prioritisation. Corporate cultures and risk-tolerance will play an important role in deciding the level of investment that will be devoted to meeting the requirements of the GDPR, but what must be taken into account are the consequences of non-compliance. These include the right to compensation for breaches for material or immaterial damage and administrative fines which are well above what has been at the disposal of regulators until now.

In terms of prioritisation, it may be useful to remind ourselves of the types of breaches that may attract the maximum level of fines under the GDPR, that is, up to 20 million euro or up to 4% of the total worldwide annual turnover, whichever is higher. These include infringements of:

- the basic principles for processing, including conditions for consent;
- the data subjects' rights;
- the conditions for lawful international data transfers;
- specific obligations under national laws, where permitted by the GDPR; and
- orders by data protection authorities, including suspension of data flows.

The next few months will be critical to prepare for compliance with what promises to be a game-changing piece of legislation. Whatever its imperfections, the GDPR is here to stay and the time for action is now.



Tougher sanctions for breach.

The GDPR and private equity – at a glance

Extra-territorial application

Enacted as a regulation therefore no further action required to implement into national law.

Single law from 25 May 2018 providing much needed consistency.

GDPR applies to the processing of data in relation to any data subject within the EU regardless of whether the data processor has a place of business in the EU.

Applies whenever the use of data relates to: the offering of goods/ services to subjects in the EU; or the monitoring of those individuals' behaviour in the EU.

Obligations of the data processors

Data processors are subject to direct obligations and liabilities for the first time.

Processors are now required to maintain records of processing activities; implement appropriate security measures; comply with international data transfer requirements; co-operate with data protection authorities; and appoint a data protection officer in some circumstances.

A sub-processor must not be appointed without authority of the controller.

The contractual obligations that you should impose on your processor (if you engage one) are much more detailed and you should review and revise any contracts with data processors.

Processors must notify the controller of any breach without undue delay.

Rights of the data subjects

The right to access.

The right to rectification.

The right to erasure.

The right to restriction of processing.

The right to data portability.

The right to object to processing.

The right to not be subject to a decision based on an automated process.

Sanctions for breach

Authorities will be able to issue fines of €20m or up to 4% of global annual turnover – whichever is higher.

Authorities can audit, issue warnings or prevent/suspend processing.

Data subjects can sue for damage (material and non-material).

Countdown to compliance 2018

Don't panic.

Plan a compliance strategy now.

Identify gaps between current requirments and GDPR or talk to Hogan Lovells' data compliance team.

Prioritise those areas of your business where GDPR will have the greatest impact.

EU GDPR - a checklist for private equity

1	Remember that even if your firm is not established in the Union, you will be subject to the Regulation if you deal with the data of individuals in the Union.
2	If you are outside the Union but are caught by the Regulation, you will need to appoint a representative in the Union (unless you are exempt).
3	Review your existing compliance policies and procedures.
4	You are unlikely to rely on 'consent' to processing and more likely to rely on the 'legitimate interests' condition in relation to your employees and investors. If you do rely on consent from any of your data subjects (for example, during fundraising) you should put in place processes to record any withdrawals of consent.
5	In light of the continuing and new rights of data subjects including to rectification, access, portability and erasure, consider the likelihood that data subjects will exercise these rights. If there is likelihood that data subjects will exercise any of their rights, put in place processes for recording and dealing with such requests.
6	Ensure your data controller records are complete and up to date.
7	Consider whether you need to appoint a data protection officer, for example if you are required to do so by the national law of the jurisdiction in which you are established; or your core activities consist of processing sensitive personal data on a large scale or regular and systematic monitoring on a large scale.
8	Update your contract templates and existing contracts (if necessary) with processors, for example data room providers.
9	Consider the extent to which you transfer data out of the EU and whether such transfers will continue to be acceptable under the GDPR.
10	Consider whether a risk assessment procedure would be beneficial and ensure your current procedures provide for reporting and dealing with breaches.
11	Contact the data protection team at Hogan Lovells if you have any queries or require any assistance in respect of any of these steps.

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Brussels
Budapest
Caracas
Colorado Springs
Denver
Dubai
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Rio de Janeiro
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar
Warsaw
Washington, D.C.
Zagreb

Our offices
Associated offices

www.hoganlovells.com